

Windows XP SP2

Line of Business
Application
Compatibility

November 3, 2003

Agenda

Kick-off	Elliot Paull
LOB App Compatibility Program	Stephanie Martin
Microsoft Java Virtual Machine (MSJVM)	Olivier D'Hose
ActiveX	Andy Dunn
Internet Connection Firewall+ (ICF+)	Michael Surkan
Windows Management Instrumentation (WMI)	Jack Creasey
Internet Explorer	Kurt Schmucker

LOB App Compatibility Program

- **Targeted applications:**

- require a client install
- web based
- use ActiveX controls
- others

<i>Shared Goals</i>	Beta Escrow	Beta	RC Escrow	RC	RTM Escrow
Ship Criteria Apps	Top 30		Top 30		Top 30
Broad Coverage Apps		150		150	

- **Team Site:**

- <http://sts/tip/windows/xpsp2lob>

- **Join the team distribution list:**

- EAP Windows XP SP2 (eapxpsp2)

- **Contact Stephanie Martin (*stephn*)**

Key Dates

LOB Test Schedule	Beta Escrow	Beta	RC Escrow	RC	RTM Escrow
Top 30 LOB Apps	Nov 7 - Nov 14		Jan/Feb 2004		TBD
150+ LOB Apps		Nov 18 - Dec 5		Feb/Mar 2004	

Note: The dates provided are dependant on the Windows product group and are for OTG planning purposes only.

- **Beta Escrow of Windows XP SP2:**
 - ICF+ OTG Pilot: Top 30 LOB applications; 150 clients in OTG
 - WMI: All clients impacted
 - IE changes
- **Post Beta 1 of Windows XP SP2:**
 - ActiveX
- **June 2004:**
 - MSJVM

Key Changes

Microsoft Java Virtual Machine (MSJVM)	Olivier D'Hose
ActiveX	Andy Dunn
Internet Connection Firewall+	Michael Surkan
Windows Management Instrumentation	Jack Creasey
Internet Explorer	Kurt Schmucker

ActiveX – Andy Dunn

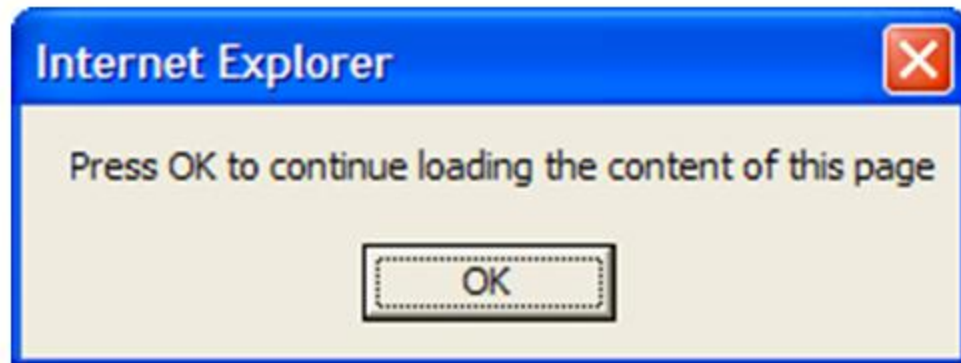
Why?

- Microsoft was ruled against in the Eolas Patent Ruling
<http://www.microsoft.com/presspass/press/2003/oct03/10-06EOLASpr.asp>
- Final judgment not yet entered
- Microsoft intends to appeal
- However, Microsoft has decided to make changes to IE to minimize or eliminate the impact during the appeal

ActiveX – Andy Dunn

What does this mean?

- If
 - you do nothing AND
 - your application uses ActiveX or Scriptlets AND
 - the ActiveX or Scriptlets access an external resource
- THEN



ActiveX – Andy Dunn

How to test this?

- <http://msdn.microsoft.com/ieupdate/>
- Install the pre release version
 - Side by side install – lives in its own directory
 - Runs alongside current release version
- Run through your app. If you don't see the dialog you are fine.

ActiveX – Andy Dunn

How to fix this (Option 1)

- <http://msdn.microsoft.com/ieupdate/activexchanges.asp>
- No <PARAM> means no prompt
- If you have <PARAM>s which don't refer to external data then tell IE
- If you have <PARAM>s that do refer to external data you can BASE64 encode them

<OBJECT **NOEXTERNALDATA="true"** CLASSID="CLSID:6BF52A52-394A-.....

<OBJECT ID="myCtrl" WIDTH=50 HEIGHT=50 CLASSID="CLSID:....." **DATA="DATA:application/x-oleobject;BASE64,j43aWGqdGxCvwEIQ">**

ActiveX – Andy Dunn

How to fix this (Option 2)

- <http://msdn.microsoft.com/ieupdate/activexchanges.asp>
- Create the object tag in script in a separate file
- e.g.

```
<HTML>
  <HEAD>
    <SCRIPT SRC="sample.js"></SCRIPT>
  </HEAD>
  <BODY>
    <SCRIPT> ReplaceContent (); </SCRIPT>
  </BODY>
</HTML>

function ReplaceContent(){
document.write('<OBJECT CLASSID="CLSID:.....">');
document.write('<PARAM NAME="URL" VALUE="http://mysite/workshop/'');
document.write('samples/author/dhtml/media/drums.wav"/></OBJECT>'); }
```

ActiveX – Andy Dunn

Other affected applications

- MSInsight
 - Uses scriptlets
 - Fixes are in v7.5 release date 11/12
 - Fixes for older versions will be available at SP2 release
- SharePoint
 - Grid view is affected.
 - They are working on a fix
 - Will ship with SP1 of SharePoint
 - If gridview is not customized you will see updated version
 - Does not affect v1.0 sites

ActiveX – Andy Dunn

Finally

- Current information is that these bits will be in the final SP2 but will NOT be in the releases during November
- Anybody got a CMS site?
- Any questions contact andydu

Internet Connection Firewall+ - Michael Surkan

- ICF+ turns XP firewall on by default
 - Now supports “Protected” mode. “Shielded” is the same as today
 - All interfaces firewalled
 - Boot-time security
 - File and Print sharing support
 - Local and domain policy support
- Protected mode allows more granular in-bound support
- Support for applications
 - Software can register with ICF+ API
 - Users/admins can specify application file names to add to allowed list
 - Need to know details about how the app works with the network to configure ICF+ properly.
- ICF+ can be managed by group policy
 - Can prevent local policy from working
 - Can configure operational mode, open ports and allowed apps
 - Can't override specific user settings (e.g. disallow opening particular ports)

Windows Management Instrumentation

- Jack Creasey

Two changes impact the use of WMI after XP SP2

- ICF+ is enabled by default. This may potentially block connections to the client.
- Security (authentication and encryption) improved for WMI namespaces which will require authentication when connecting to client.

Windows Management Instrumentation

- Jack Creasey

ICF+ Issues

- How are ICF Settings are implemented/disabled via GPO ?
 - XPSP2 will contain .adm for policy setup
- Can SMS still push down packages to clients?
 - Required ports must be opened
- Can MOM acquire data from the clients?
- Required ports must be opened
- What transport (TCP/UDP/RPC) does your server use to contact the client?
 - OTG need to catalog connection needs to client

Windows Management Instrumentation

- Jack Creasey

WMI Namespace security and Encryption

- Not turned on by default
 - Requires addition of a registry entry in the WBEM key
 - HKEY_Local_Machine\Software\Microsoft\WBEM\CIMOM
 - Add key RequiresEncryptedConnection
- PG want us to turn this on
 - Means we have to configure feature in client after XPSP2 deployment
 - Means updating scripts

Internet Explorer - Kurt Schmucker

Goals:

- Eliminate IE viruses by mitigating elevation of privilege threats
- *"Where ever I go with IE, I will be safe until I explicitly download more code."*

Internet Explorer - Kurt Schmucker

Some App Compat issues possible:

- Local Machine Zone protections
- Filetype security checks for file downloads
- No binary behaviors in Restricted Zones (impact for HTML mail)

Internet Explorer - Kurt Schmucker

Few App Compat issues possible:

- UI Spoofing prevention
- Bind to Object ActiveX security checks

Internet Explorer - Kurt Schmucker

No App Compat issues expected:

- Download prompt UI
- Pop-up window manager
- Java Hardening
- Buffer overrun mitigations
- Restrict ChangeMyHomePage()

Appendix - Testing Instructions

- **MSJVM:** Contact olivierd if 3rd party app and in negotiation; Additional details/instructions to come.
- **ActiveX:** Follow instructions on <http://msdn.microsoft.com/ieupdate/>
- **Internet Connection Firewall+ Pilot**
 1. ICF+ on by default for machines in ICF+ Pilot Security Group
 2. Turn ICF+ off manually
 3. Test applications
 4. Turn on ICF+ manually
 5. Test applications again
 6. If blocked, open ports with ICF+, report back to *stephn* any port number (and port's purpose) that need opening.
 7. Test application again
 8. If still blocked, escalate to *stephn* immediately.
- **WMI:** Test app as usual
- **IE:** Test app as usual; Special focus on Local Machine Zone; Hooks for testers available for most changes

Microsoft®

StreamLine

Live Streaming and Archiving by:

StreamLine

***See the Guide at
HTTP://MSRN***

Can we cover your event?

StreamIt@microsoft.com